

**Sensitive Information on Excessed Computers
Needs To Be More Effectively Safeguarded**

March 2002

Reference Number: 2002-20-074

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

March 29, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

A handwritten signature in cursive script, reading "Pamela J. Gardiner".

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Sensitive Information on Excessed
Computers Needs To Be More Effectively Safeguarded
(Audit # 200120039)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) policies and procedures for handling sensitive information¹ on excessed computer equipment.²

In summary, the IRS collects, maintains, uses, and disseminates tax returns and related information as required under the law. Therefore, the IRS has a legal obligation to protect the confidentiality of the information entrusted to it, including the responsibility to protect computer equipment and any information stored on it. The IRS has established that, before excessed computer equipment is reused, transferred, or discarded, sensitive information must be removed. Between September 30, 2000, and September 5, 2001, the IRS excessed 27,863 computer equipment items including 6,491 personal computers.³

The IRS' Information Technology Services, Operations Support Office is responsible for ensuring the adherence to procedures requiring the removal of sensitive information from excessed computers before equipment disposal. The IRS is currently conducting training to communicate the policies and procedures governing secure data destruction

¹ Any information (including tax and tax-related information) which, if released without proper authorization, could adversely affect IRS operations; all information processed by the IRS is considered sensitive.

² Any Automated Data Processing property under the control of any Federal agency that is not required for the fulfillment of the agency's needs, as determined by the head of the agency.

³ Includes microcomputers (5,004), laptops (1,403), and servers (84).

to employees and to standardize the tools used to remove information from excessed computers. However, improvements are needed in the management of excessed computers to ensure sensitive information is properly removed. The IRS approved the usage of overwrite software⁴ and degaussing equipment⁵ for the removal of sensitive information from excessed computers, but the tools were not always available or were not always used consistently at the five sites we visited. As a result, offices have used unapproved and inconsistent methods and have spent unnecessary resources.

In addition, personnel were not following established procedures. In seven instances information was not wiped from excessed computers before the computers were reassigned to another employee or slated to leave the IRS sites. By not consistently implementing established procedures and using authorized tools to remove sensitive information from excessed computers, the IRS has increased its risk of disclosure of sensitive information and increased program administration costs.

The Deputy Commissioner for Modernization & Chief Information Officer should ensure specific personnel are designated with responsibility for ensuring procedures are followed at each IRS site. Further, these employees should be provided the necessary tools to ensure sensitive information is properly removed from excessed computers and adequately trained in the use of these tools.

Management's Response: Management's response was due on March 29, 2002. As of that date, management had not responded to the draft report.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

⁴ Overwrite software writes non-sensitive information over sensitive information.

⁵ Degaussing equipment removes information by erasure (demagnetization).

**Sensitive Information on Excessed Computers
Needs To Be More Effectively Safeguarded**

Table of Contents

Background	Page 1
The Internal Revenue Service Has No Assurance That Sensitive Information Is Properly Removed From Excessed Computers	Page 2
<u>Recommendations 1 and 2:</u>	Page 5
Appendix I – Detailed Objective, Scope, and Methodology	Page 6
Appendix II – Major Contributors to This Report.....	Page 8
Appendix III – Report Distribution List	Page 9
Appendix IV – Outcome Measures	Page 10

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

Background

The Internal Revenue Service (IRS) collects, maintains, uses, and disseminates tax returns and related information as required under the law. Therefore, the IRS has a legal obligation to protect the confidentiality of the information entrusted to it, including the responsibility to protect computer equipment and any information stored on it. In its Fiscal Year (FY) 2000 – 2005 IRS Strategic Plan, the IRS cites its strategy to provide effective stewardship of information by improving internal processes for information management. As part of this strategy, the IRS has established that, before excessed computer equipment¹ is reused, transferred, or discarded, sensitive information² must be removed by either overwriting or degaussing. Between September 30, 2000, and September 5, 2001, the IRS excessed 27,863 computer equipment items including 6,491 personal computers.³

Overwriting is a process whereby non-sensitive information is written over sensitive information using software that overwrites with a pattern, then its counterpart, and finally with another pattern (e.g., overwrite first with 0011 0101, followed by 1100 1010, then 1001 0111). Degaussing involves using a National Security Agency-approved degausser to remove the information by erasure (demagnetization).

Audit work was conducted at the IRS' National Headquarters locations, the Memphis IRS Center/ Tennessee Computing Center and the Atlanta, Baltimore, and Nashville territory offices during September through December 2001. This audit was scheduled as part of the Treasury Inspector General for Tax Administration's FY 2002 Annual Audit Plan and was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology

¹ Any Automated Data Processing property under the control of any Federal agency that is not required for the fulfillment of the agency's needs, as determined by the head of the agency.

² Any information (including tax and tax-related information) which, if released without proper authorization, could adversely affect IRS operations. All information processed by the IRS is considered sensitive.

³ Includes microcomputers (5,004), laptops (1,403), and servers (84).

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

The Internal Revenue Service Has No Assurance That Sensitive Information Is Properly Removed From Excessed Computers

is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The Office of Management and Budget Circular A-130 requires the head of each federal agency to ensure that agency data (automated information) are adequately secured. This responsibility includes establishing physical, administrative, and technical safeguards to protect personal, proprietary, or other sensitive information. The IRS' Information Technology Services, Operations Support Office is responsible for ensuring the adherence to procedures regarding data security and magnetic media handling. IRS procedures require the removal of information contained on excessed computers by overwriting or properly degaussing sensitive information before removing the excessed computer equipment from an IRS site. Other techniques (e.g., reformatting⁴) are not considered acceptable because data can still be recovered using existing data recovery tools.

The IRS is currently conducting training to communicate the policies and procedures governing secure data destruction to employees and to standardize the tools used to remove information from excessed computers. This training is scheduled to be completed by September 30, 2002. In coordination with the training initiative, nationwide procedural guidance was updated effective January 1, 2002, outlining the operating procedures to be implemented to ensure the removal of sensitive information from computers. However, improvements are needed in the management of excessed computers to ensure sensitive information is properly removed.

Tools approved for the removal of sensitive information were not always available or were not always used consistently

Four of the five sites we visited were not using the required overwrite software and/or an approved degausser to remove sensitive information from excessed computers. As a result,

⁴ Reformatting erases a disk's address tables but does not erase the data.

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

offices have used unapproved and inconsistent methods and have spent unnecessary resources. For example:

- One site had a degausser but was not using overwrite software. Site personnel spent approximately 3 weeks, over several months, at a cost of approximately \$1,900 manually removing all hard disks from the computers to prepare the disks for degaussing. Despite the expenditure of these resources, the sensitive information was not removed from the disks because the degausser was inoperable. We observed approximately 1,000 hard disks waiting to be degaussed. The IRS could save the cost of manually removing hard disks by using overwrite software.
- Two of the sites used overwrite software but had no degausser. One site paid a vendor \$75 per hour to physically alter (by bending) hard disks they could not overwrite. The site then designated these altered disks for offsite destruction although the data had not been properly removed. We observed 186 hard disks that the vendor had physically altered at an estimated cost of \$4,650. The IRS could save the cost to physically alter the hard disks if their employees used a degausser to remove sensitive data. The second site used a drill press to drill holes through hard disks it could not overwrite, in an attempt to make the information unrecoverable before throwing the disks away.
- One site did not use overwrite software or have a degausser. Personnel reformatted the hard disks in an attempt to make the information unrecoverable and then sent the disks offsite for degaussing. Testing of one of the reformatted hard disks with data recovery software identified legible words still stored on the disk.

Only one of the five sites visited had both tools. At that site, we identified one instance where personnel did not use either tool to remove information from an excessed laptop computer. Instead, personnel used a hammer to break the hard disk before throwing it away.

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

The four sites discussed above (bulleted) did not use or did not have the tools necessary to remove sensitive information from excessed computers because site personnel did not know that the tools were available to them, management did not approve requests for the tools, and a malfunctioning tool was not timely fixed.

Procedures for removing sensitive information were not being followed

IRS procedures provide guidance on how employees should remove sensitive information from excessed computers and conduct quality reviews of degaussed computers. However, at all five sites visited, personnel were not following established procedures because there was no clear accountability for ensuring IRS personnel strictly adhere to them. We identified or learned of seven instances, at two sites, where information was not wiped from excessed computers before the computers were reassigned to another employee or slated to leave the IRS sites.

- At one site, the site director's sensitive personnel-related information was found on a computer that was taken from the warehouse and assigned to a new employee. Also, at the same site, we found two unwiped electronic filing unit computers⁵ on warehouse pallets of excessed computer equipment labeled for offsite destruction. In addition, in the site's warehouse, we found three unwiped laptop computers on pallets labeled for offsite destruction.
- As previously reported, employees at one site that did not use overwrite software or have a degausser were reformatting the hard disks on its excessed computers. We were able to recover legible words stored on one of the reformatted computers slated to leave the site.

In addition, two of the five sites we visited had a degausser onsite and, per IRS guidelines, site personnel are required to conduct quality reviews on 10 percent of the degaussed hard

⁵ Site personnel wiped these two computers before we could test them.

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

disks. At the first site, personnel advised us that they reviewed some of the degaussed disks, but a 10 percent sample was not quality reviewed as required. At the second site, instead of quality reviewing degaussed disks, personnel drilled a hole through the disks and sent them offsite to be destroyed. The required reviews were not conducted because personnel were unaware of the requirement.

By not consistently implementing established procedures and using authorized tools to remove sensitive information from excessed computers, the IRS has increased its risk that sensitive information will be inappropriately disclosed. Unauthorized disclosure of tax and tax-related information could result in lawsuits, unwanted notoriety, and public distrust due to the IRS' inability to protect such information. In addition, the IRS is incurring increased costs because it is paying a vendor to bend excessed computer disks and paying employees to remove disks from excessed computers to prepare them for degaussing.

Recommendations

The Deputy Commissioner for Modernization & Chief Information Officer should:

1. Designate appropriate personnel responsible for each IRS site to ensure procedures are followed to properly remove information from excessed computers and to conduct the required quality reviews.

Management's Response: Management's response was due on March 29, 2002. As of that date, management had not responded to the draft report.

2. Ensure the designated personnel are equipped with and trained to use the approved overwrite software and an approved degausser for removing information from the excessed computers.

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine the effectiveness of the Internal Revenue Service's (IRS) policies and procedures for handling sensitive information¹ on excessed computer equipment.² To accomplish this objective, we:

- I. Evaluated IRS' policies and procedures for removal/disposal of sensitive information on excessed equipment.
 - A. Reviewed the Internal Revenue Manual and other guidelines to identify policies and procedures for excessing computer equipment.
 - B. Interviewed Information Technology Services and, as necessary, Facilities Management personnel responsible for removal and disposal of sensitive information on the computer equipment to determine how the procedures had been implemented and did a walk-through of the disposal process.
- II. Reviewed Information Technology Asset Management System (ITAMS) information to identify computer equipment items no longer in service/retired.
 - A. Obtained a download of the ITAMS database information as of September 5, 2001.
 - B. Using the ITAMS data, identified 27,863 equipment items with retirement dates falling in Fiscal Year 2001.
 1. Sorted the data based on equipment type and volume (e.g., computers, laptops, and servers).
 2. Sorted the data based on disposal code (e.g., for disposal code 06 representing a donated asset).
- III. Selected a sample of the equipment that had been designated as excessed and determined whether the equipment contained sensitive information.
 - A. Visited 5 of 14 IRS sites with over 500 retired equipment items in FY 2001. The sites were identified through our data sorts of the ITAMS data in step II.B. A judgmental sample of the sites to visit was selected because the results were not going to be projected to the entire population.

¹ Any information (including tax and tax-related information) which, if released without proper authorization, could adversely affect IRS operations. All information processed by the IRS is considered sensitive.

² Any Automated Data Processing property under the control of any Federal agency that is not required for the fulfillment of the agency's needs, as determined by the head of the agency.

**Sensitive Information on Excessed Computers
Needs To Be More Effectively Safeguarded**

- B. Selected a judgmental sample of one or more excessed computer equipment items for review based on the number of items available for review at the time of our site visit. A judgmental sample was selected because the results were not going to be projected to the entire population.
- C. Obtained collateral assistance from the Treasury Inspector General for Tax Administration's Office of Investigations to determine whether the sample items contained sensitive information by using data recovery software.
- D. Calculated the number of sampled excessed computer equipment items that contained sensitive information (identified in step III.C.).

**Sensitive Information on Excessed Computers
Needs To Be More Effectively Safeguarded**

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Danny Verneuille, Audit Manager
Kevin Burke, Senior Auditor
Mark Carder, Auditor

**Sensitive Information on Excessed Computers
Needs To Be More Effectively Safeguarded**

Appendix III

Report Distribution List

Commissioner N:C
Deputy commissioner N:DC
Chief, Agency-Wide Shared Services A
Chief, Information Technology Services M:I
Director, Real Estate and Facilities Management A:RE
Director, Strategic Planning and Client Services M:SP
Director, Enterprise Operations M:I:E
Director, End User Equipment and Services M:I:F
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaisons:
 Deputy Commissioner for Modernization & Chief Information Officer M
 Office of Program Oversight and Coordination M:SP:P:O
 Chief, Agency-Wide Shared Services A

Sensitive Information on Excessed Computers Needs To Be More Effectively Safeguarded

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to the Congress.

Type and Value of Outcome Measure:

- Cost Savings, Recommendations That Funds Be Put to Better Use – Potential; \$4,650 for a vendor to physically alter (by bending) 186 hard disks from excessed computer equipment¹ (see page 2).

Methodology Used to Measure the Reported Benefit:

At one of the sites visited, we observed 186 hard disks that a vendor had physically altered (by bending). We requested supporting invoices itemizing the charges for altering the disks; however, we received only one invoice itemizing this type of work and it did not state the number of disks altered or the specific charges for altering the disks. Therefore, we calculated an estimated cost for altering the disks based on the following information:

- Vendor's hourly rate: \$75 per hour.
- Estimated amount of time to alter a disk: 20 minutes per disk (estimate provided by the IRS).
- Number of disks altered: 186.

Estimated vendor cost to alter the 186 disks:

186 disks * 20 minutes (estimated) per disk / 60 minutes per hour = 62 estimated hours of work.

62 estimated hours of work * \$75 per hour (vendor's hourly rate) = **\$4,650.**

¹ Any Automated Data Processing property under the control of any Federal agency that is not required for the fulfillment of the agency's needs, as determined by the head of the agency.